一种基于秘密分享的高质量(k,n)可视加密算法 *

丁海洋 [1,2]

(1. 北京印刷学院 信息工程学院，北京 102600; 2. 北京邮电大学 信息安全中心，北京 100876)

摘　要：(k，n)可视加密算法是一种重要的信息隐藏算法。应用 Shamir 秘密分享的概念，将一幅二进制秘密图像隐藏在 n 幅分享图像中，通过在分享过程中增加随机性控制，保证生成的分享图像是接近噪声图像的无意义图像。从 n 幅无意义分享图像中，任意选取 k 幅分享图像，使用拉格朗日插值可提取秘密图像。该算法应用 Shamir 秘密分享来实现(k，n)可视加密，不需要码书，不会造成无限制的像素扩展。实验结果显示，该算法能实现(k，n)可视加密，提取秘密图像的提取正确率能保证 100%。

关键词：Shamir 秘密分享；(k，n)可视加密；拉格朗日插值

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2017.12.1044

High quality (k,n) visual cryptography based on secret sharing

Ding Haiyang[1,2]

(1. *College of Information Engineering*, *Beijing Institute of Graphic Communication*, *Beijing* 102600, *China*; 2. *Information Security Center*, *Beijing University of Posts & Telecommunications*, *Beijing* 100876, *China*)

Abstract: (K, n) visual cryptography is an important data hiding algorithm. Using Shamir's secret sharing, a binary secret image can be shared into n meaningless shares, in order to make the generated shares more like noise images, adding the randomness within the process of sharing. Picking any k shares from n meaningless shares, the secret image can be revealed by using Lagrange interpolation. This paper applied Shamir's secret sharing to realize a (k, n) visual cryptography, and this method neither required code book nor suffers from pixel expansion. Experimental results show the proposed method can realize a (k, n) visual cryptography, and correct decoding rate (CDR) of revealed secret image can be guaranteed.

Key words: Shamir's secret sharing; (k,n) visual cryptography; Lagrange interpolation

0　引言

可视加密(VC)的概念最早出现在 Naor 和 Shamir 的文献[1]中。这里提出一个(k,n) VC 的概念，即将一幅秘密图像隐藏在 n 幅图像中，任意取得 k 幅图像，则可提取出秘密图像。在文献[2,3]中提出扩展可视加密的算法；Hou 等人[4]提出一种友好的可视加密，将秘密图像隐藏在两幅图像中；Yan 等人[5]提出一种基于纠错码的信息隐藏算法。以上算法[1~5]都属于基于像素扩展的可视加密，这类算法实现简单，并可产生无意义的分享图像，但是它的主要缺点是像素扩展和需要码书，随着用户数的增加，分享图像的分辨率将会被扩大很多倍。

基于随机网格的可视加密，即采用随机网格技术产生无意义分享图像，不会造成像素扩展。Kafri 等人[6]给出随机网格的最初概念，并提出三种信息隐藏的方法。Chen 等人[7]提出(2,n)情况下的基于随机网格的可视加密；Chen 等人在文献[8]中提出(k,n)情况下的基于随机网格的可视加密。文献[9,10]则描述基于随机网格的可视加密的通用形式。Ou 等人[11]提出一种基于随机网格的标签可视加密。Yan 等人[12]提出一种基于随机网格的可视秘密分享算法，该算法采用通用接口结构和多重解密。Rabari 等人[13]提出扩展的(2,m,n)随机网格可视加密算法，该算法可以应用到灰度和彩色图像。基于随机网格的可视加密[6~13]，主要优点是不需要码书，不会造成像素扩展，可以生成无意义分享图像；但是这类算法的主要缺点是提取的秘密图像对比度太低，很多情况下对比度低于 1/10，很难提取出一幅清晰的秘密图像。

近年来，基于图像分块的可视加密逐渐称为一个新的研究方向。Hou 等人[14]提出一种基于图像分块的(2,n)可视加密算法，一幅秘密图像可以被分解为 n 个不相重叠的图像块，基于这些图像块生成 n 幅分享图像，只要获取任意 k(2≤k≤n)个分享，则可提取出部分图像块。但是 Hou 等人的算法[14]可能会发生欺骗问题。Hou 等人[15]提出一种欺骗免疫的基于图像分块的(2,n)可视加密算法。另外，Roy 等人[16]提出一种(3,4)秘密图像分享，将秘密图像中每个 2×2 的图像块，分解为 4 种组合，分享到 4 个分享图像中，只要获取任意 3 个分享，则可恢复出秘密图像。

收稿日期：2017-12-21；**修回日期：**2018-03-23　**基金项目：**北京市教委科研计划一般项目（KM201610015002）；国家自然科学基金资助项目（61370188）；北京市教委科研计划重点项目（KZ201710015010）；科技创新服务能力建设-科研水平提高定额项目（PXM2017_014223_000063）

作者简介：丁海洋（1979-），男，黑龙江哈尔滨人，讲师，博士，主要研究方向为信息隐藏、半色调信息隐藏、数字图像处理（o_dhy@163.com）.

基于图像分块的可视加密[14~16]，主要优点是不需要码书和计算复杂度低，并能产生无意义分享图像；但是其主要缺点是，k 个分享只能恢复秘密图像的一部分，假如 n 的数目发生变化，需要对秘密图像进行重新分块。

通过表 1 列出各类可视加密算法的比较。

表 1　不同可视加密 (VC) 算法的对比

算法名称和参考文献	优点 (+)	缺点 (-)
基于像素扩展的 VC [1-5]	+ 低计算复杂度	- 像素扩展 - 需要码书
基于随机网格的 VC [6-13]	+ 没有像素扩展 + 不需要码书	- 提取秘密图像的对比度太低 - 很难提取清晰的秘密图像
基于图像分块的 VC [14-16]	+ 不需要码书 + 低计算复杂度	- k 个分享只能恢复部分秘密图像 - 假如 n 的数目发生变化，需要对秘密图像进行重新分块。

本文的目标是研究一种高质量(k,n)可视加密算法，该算法不需要码书，不会造成无限制的像素扩展。本文使用 Shamir 秘密分享的概念为基础，一个秘密数据 D 可分享为 n 块数据，任意选取 n 块数据，则可以恢复数据 D。

本文提出一种基于 Shamir 秘密分享的高质量(k,n)可视加密算法。使用该算法，将一幅二进制秘密图像隐藏在 n 幅分享图像中，通过在分享过程中增加随机性控制，保证生成的分享图像是接近噪声图像的无意义图像。从 n 幅无意义分享图像中，任意选取 k 幅分享图像，使用拉格朗日插值可提取秘密图像。

1　Shamir 秘密分享

在 Shamir 的文献[17]中，提出一种(k,n)门限秘密分享算法。将一个秘密信息 D，生成 n 个分享数据 $D_1,\dots,D_n$，从这 n 个分享中，任意取得 k 个数据，可计算得到原始数据 D。具体过程：

定义一个 k-1 次多项式 $q(x)$，如式（1）所示。另 a_0=D，任意选取系数 $a_1,\dots,a_{k-1}$，对 n 个输入值 $x_1,\dots,x_n$，分别计算 $D_1=q(x_1),\dots,D_n=q(x_n)$，可产生 n 组分享数据$(x_1,D_1),\dots,(x_n,D_n)$，只要获取 k 组分享数据，可通过计算拉格朗日插值得到秘密数据 D。

$$q(x)=a_0+a_1x+a_2x^2+a_3x^3+\dots+a_{k-1}x^{k-1} \quad (1)$$

需要注意四个问题：

a)选择一个素数 p，$D,a_1,\dots,a_{k-1}$ 和 n 的数据范围都是[0,p)；

b)分享数据 x_i 和 y_i 的数据范围也在[0,p)，所以计算 y_i 时需要 modp；

c)如果秘密数据 D 很大，可将数据 D 分为多个 mbit 构成的分块数据；

d)对不同的秘密数据 D，可使用不同多项式生成分享数据。

2　使用 Shamir 秘密分享实现秘密图像分享

参考 Shamir 秘密分享[17]，一幅秘密图像不能直接作为一个秘密数据，必须先被分解为多个 mbit 分块。每个 mbit 的分块作为一个秘密数据 D，使用一个 k-1 次的多项式 f(x)，另 a_0=D，分别计算 $y_i=f(x_i)$，产生 n 组分享数据$(x_1,y_1),\dots,(x_n,y_n)$，将 n 组分享数据分别存到 n 幅分享图像的对应位置。在整幅秘密图像上完成以上分享过程后，可生成 n 幅分享图像。

但是，实现这个分享过程中，需要注意以下三个问题：

a）数据位数 m 的选择；

b）主要数据的范围；

c）增加随机性控制。

2.1　数据位数 m 的选择

将 mbit 数据作为一个秘密数据 D，则 D 的范围是$[0,2^m-1]$，用户数目 n 需要小于等于 2^m-1。那么，如何选择数据位数 m 呢？

从安全角度，数据位数越大越安全，但由于半色调信息隐藏中，存在一定误码，如果数据位数 m 太大，会造成整体秘密图像的误码率太高；如果数据位数 m 太小，则可容纳的用户数 n 会很小。所以，在本文中，选择数据位数 m=4，即每 4bit 数据为一个秘密数据 D，则 D 的范围是$[0,15]$。

2.2　主要数据的范围

a）因为 m=4，所以 a_0 范围为$[0,15]$；

b）p 是一个素数，而且 $p>2^m-1$，所以 p=17；

c）x_i 的范围是$[0,15]$，但是 $x_i=0$ 时，$y_i=a_0$，表示 a_0 没有被隐藏，因此 $x_i\neq0$，所以 x_i 范围为$[1,15]$；

d）y_i 的范围是$[0,15]$；

e）用户数目 n 小于等于 15，k 则小于 n。

2.3　无随机性控制下的秘密图像分享

2.3.1 无随机性控制下的秘密图像分享过程

结合 2.1 和 2.2 节给出无随机性控制下的秘密图像分享流程，如图 1 所示，通过分享过程，可将一幅秘密图像 S 分享为 n 幅无意义分享图像。具体流程如下：

a）生成一个 k-1 次多项式 f(x)。

b）使用多项式 f(x)生成多组可选数据，并选择可用数据。

(a)由 2.2 节已知，a_0 范围为$[0,15]$，x_i 的范围为$[1,15]$，y_i 的范围为$[0,15]$，且 p=17。

(b)使用式（2），分别带入 x_i 的 15 个值，计算生成 15 组数据(x_i,y_i)。

$$y=(a_0+a_1x+a_2x^2+a_3x^3+\dots+a_{k-1}x^{k-1}) \bmod p \quad (2)$$

(c)因为数据位数 m=4，需要使用式(3)去除 y_i=16 的数据：

$$\begin{cases}(x_i, y_i)\ \text{可用} & y_i \neq 16 \\ (x_i, y_i)\ \text{不可用} & y_i = 16\end{cases} \tag{3}$$

(d)对可用数据，使用式（4）计算 $NumofOne_i$。$NumofOne_i$ 表示第 i 组数据(x_i,y_i)中比特值为 1 的数目，将可用数据根据$|NumofOne_i-4|$的数值从小到大排序，选择前 n 组数据，作为分享数据。排序的目的：在可用数据中优先选择 0 和 1 数目相等的数据，这样生成的分享图像更接近于无意义图像。

(e)通过以上过程，得到的数据结构形式：$array(a_0,x_i,y_i)$，其中 i=1:n，表示对每个 a_0 值对应的 n 组分享数据(x_i,y_i)。

$$NumofOne_i = \sum_{b=0}^{3} getbit(x_i, b) + \sum_{b=0}^{3} getbit(y_i, b) \tag{4}$$

c）秘密图像 S 分辨率为 $W\times H$，将 S 分解为 $W/4\times H$ 组 4bit 数据，每组 4 bit 数据 $B_{i,j}$ 作为一个秘密数据 D，其中 i=0:(W/4-1)，j=0:(H-1)，使用式（5）计算 $B_{i,j}$ 对应的秘密数据值 $S_{i,j}$。

$$S_{i,j} = \sum_{b=0}^{3} B_{i,j}(b) \times 2^b \tag{5}$$

d）另 $a_0=S_{i,j}$，从 b）中的 $array(a_0,x_i,y_i)$数组中找到当前 a_0 值对应的 n 组数据(x_i,y_i)，将 n 组数据分享到 n 个分享图像对应位置，即将(x_i,y_i)分解为 8bit 二进制数，生成第 i 个分享图像对应位置的像素。

e）通过上述过程，将一幅秘密图像 S 分享为 n 幅无意义分享图像，每幅分享图像分辨率为 $2W\times H$。

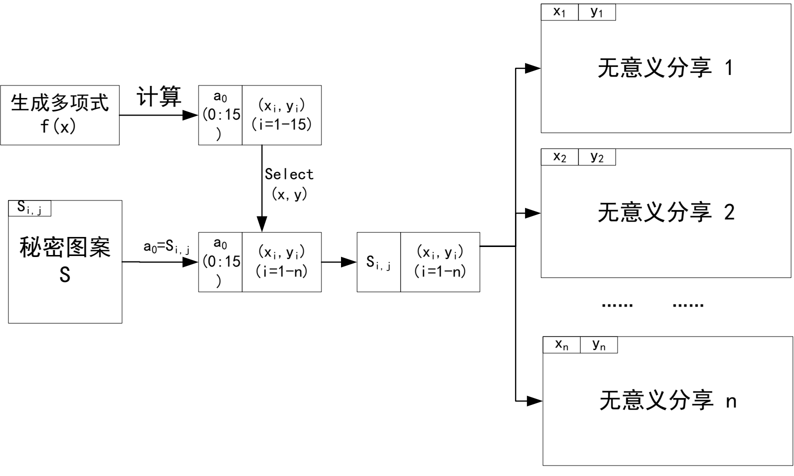


图 1 无随机性控制下的秘密分享过程

2.3.2 秘密图像分享的实现效果

图 2 为秘密图像 S，图像分辨率均为 256×256。

使用 2.3.1 节中的方法，以图 2(a)为秘密图像 S，实现(3,4)分享模型，即将秘密图像 S 分享到 4 幅分享图像中，获取任意 3 幅分享图像，则可恢复秘密图像 S。具体过程如下：

BUPT BIGC
BUPT BIGC

(a) BUPT (b) BIGC

图 2 秘密图像 S

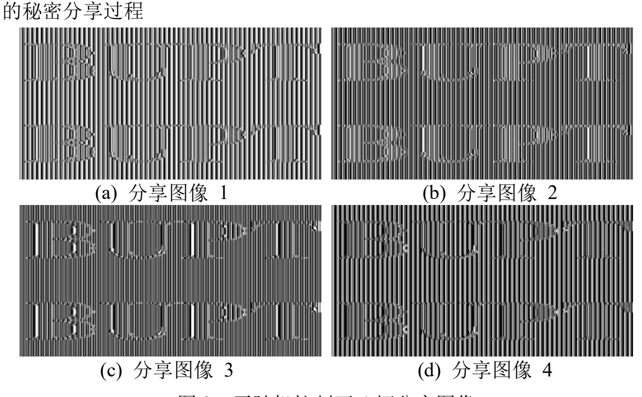
a）生成一个二次多项式，设 $a_1=1,a_2=2$，则多项式 $f(x)=a_0+1*x+2*x^2$；

b）使用 f(x)生成可用数据数组：$array(a_0,x_i,y_i)$；

c）将秘密图像 S 分解为 64×256 组 4bit 数据，使用式（5）计算 $S_{i,j}$；

d）另 $a_0=S_{i,j}$，从 b）中的 array 数组中找到当前 a_0 值对应的 4 组数据(x_i,y_i)，将 4 组数据分享到 4 个分享图像对应位置。

由于秘密图像 S 是 256×256，每组 4 bit 数据 $B_{i,j}$ 生成 4 组分享数据(x_i,y_i)，每组(x_i,y_i)共 8 bit，所以分享后的图像分辨率为 512×256。



(a) 分享图像 1 (b) 分享图像 2

(c) 分享图像 3 (d) 分享图像 4

图 3 无随机控制下 4 幅分享图像

通过上述过程，生成 4 幅分享图见图 3。从图 3 可看出，分享效果不好，能看出秘密图像，达不到秘密隐藏的要求。

2.3.3 原因分析

在上面的分享过程中存在三方面的规律性：

a）如果秘密图像 S 中数据变化较少，且有规律，会造成很多连续相同的 a_0，例如：连续的 $a_0=15$，连续的 $a_0=0$，且 a_0 的变化会反映秘密图像的变化；

b）用相同 f(x)和相同 a_0 值，生成的 4 个分享数据必然相同；

c）4 组分享数据存放到 4 幅分享图像的顺序固定。

由于这三方面的规律性，造成图 3 中分享图像的问题。a）中的规律性由秘密图像 S 造成，不能进行人为控制；b）和 c）

中的规律性都是由算法设计造成，可通过增加随机性控制来改进。

2.4 秘密分享过程中增加随机性控制

2.4.1 随机性控制的选择

根据 2.3.3 节中的分析，可通过三方面增加随机性控制：

a）使用多个生成多项式，不同的秘密数据使用不同多项式；

b）每个多项式针对每个 a_0，生成超过 n 组的可用数据，从中任选 n 组数据作为分享数据；

c）增加分享数据存放的随机性，使得分享数据存放顺序不固定。

2.4.2 增加随机性控制

在分享过程中增加随机性控制，包括三个方面：

a)使用多个多项式。初始化 *pm* 个 *k-1* 次多项式 $f_1(x),\ldots,f_{pm}(x)$，每组 4 bit 秘密数据 D，可随机选择多项式 $f_r(x)$，另 $a_0=D$ 生成分享数据；

b）生成多组分享数据。使用多项式 $f_r(x)$生成 *n+expnum* 组分享数据，从 *n+expnum* 组分享数据中选择 n 组分享数据，可有 $C_{n+\text{expnum}}^{n}$ 种组合；

c）增加分享数据存放的随机性。在将 *n* 组数据存放到分享图像前，生成一个 *[0,(n-1)]* 的随机数 *cshift*，计算 $c_i=(i+cshift) \bmod n$，将第 i 组分享数据(x_i,y_i)存放到第 c_i 幅分享图像的对应位置。

增加上述随机性后，通过多项式生成的数据结构形式为：$array(pnum,a_0,x_i,y_i)$，表示第 *pnum* 个多项式，与 a_0 值对应的 *n+expnum* 组分享数据(x_i,y_i)。

2.4.3 实验效果

以图 2(a)为秘密图像 S，实现(3,4)分享模型，为对比实验效果，分别使用不同的随机性控制，生成的分享图像见图 4~6。

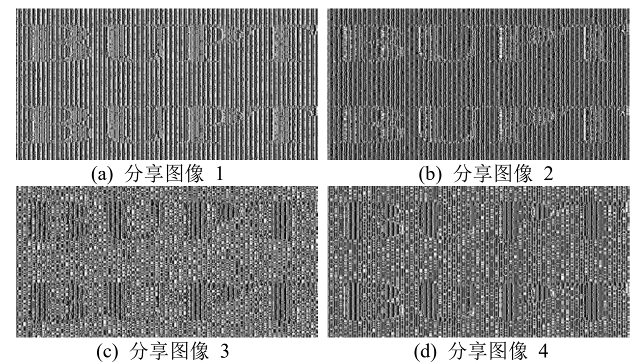

(a) 分享图像 1　(b) 分享图像 2
(c) 分享图像 3　(d) 分享图像 4
图 4　一个多项式和 n+expnum 组实验数据生成的分享图像

图 4 中，仍采用一个多项式，生成 *n+expnum* 组实验数据，其中 *n*=4，*expnum*=2，从中选择 n 组实验数据生成分享图像。从图 4 可看出，增加实验数据的随机性，效果好一些，但仍能看出秘密图像的轮廓。

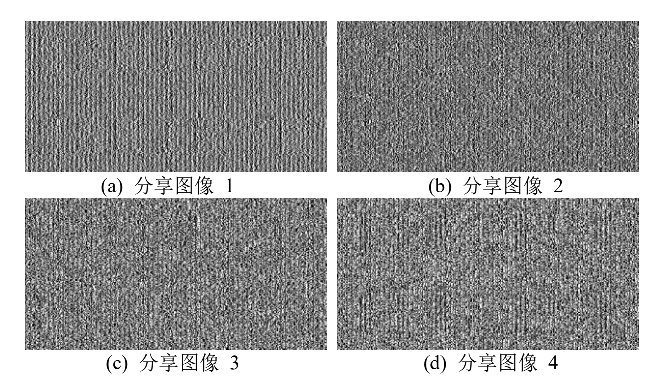

(a) 分享图像 1　(b) 分享图像 2
(c) 分享图像 3　(d) 分享图像 4
图 5　pm 个多项式和 n+expnum 组实验数据生成的分享图像

图 5 中，采用 *pm* 个多项式，生成 *n+expnum* 组实验数据，其中 *pm=6*，*n=4*，*expnum=2*，从中选择 n 组实验数据生成分享图像。从图 5 可看出，增加多项式随机性，分享图像中无法看出秘密图像，但 4 幅分享图像分布明显不均匀。

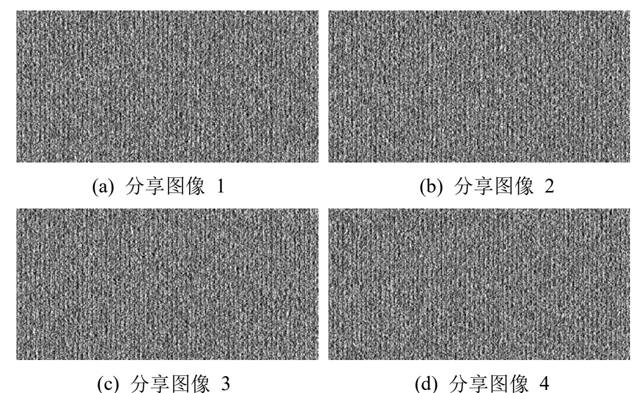

(a) 分享图像 1　(b) 分享图像 2
(c) 分享图像 3　(d) 分享图像 4
图 6　三种随机控制下生成的分享图像

图 6 中，采用 *pm* 个多项式，生成 *n+expnum* 组实验数据，其中 *pm*=6，*n*=4，*expnum*=2，增加分享数据存放顺序随机性。图 6 可看出，增加分享数据存放顺序随机性，分享图像中不仅无法看出秘密图像，且 4 幅分享图像分布均匀。

通过上面的实验可以看出，通过上述三种随机性控制组合使用，实现分享图像效果最好。本文将在第 3 章给出将秘密图像生成 n 个分享图像的完整过程。

3 本文提出的算法

本文提出一种基于 Shamir 秘密分享的高质量(k,n)可视加密算法。使用该算法，将一幅二进制秘密图像分享为 n 幅无意义图像，从 n 幅分享图像中任意选取 k 幅分享图像，使用拉格朗日插值可提取秘密图像。

3.1 一幅秘密图像被分享为 n 幅无意义分享图像

基于第 2 章的内容，使用 Shamir 秘密分享，将一幅秘密图像 S 分享为 n 幅无意义分享图像，实现流程见图 7。主要包括：

a）生成 pm 个 k-1 次多项式 $f_1(x),\ldots,f_{pm}(x)$。

b）使用每个多项式 $f_r(x)$（r=1:pm）针对每个 a_0 值生成并选择可用分享数据。

(a)由 2.2 已知，a_0 范围为[0,15]，x_i 的范围为[1,15]，y_i 的范围为[0,15]，且 p=17。

(b)使用式（2），分别带入 x_i 的 15 个值，计算生成 15 组数据(x_i,y_i)。

(c)数据位数 m=4，使用式（3）去除 y_i=16 的数据。

(d)对可用数据，使用式（4）计算 $NumofOne_i$，将有效数据根据$|NumofOne_i-4|$的数值从小到大排序，选择前 *n+expnum* 组数据，作为分享数据。

(e)通过以上过程，得到的数据结构形式：$array(pnum,a_0,x_i,y_i)$，其中 *pnum=1:pm*，$a_0=0:15$，*i=1:(n+expnum)*。图 7 中简写为 *i=1:(n+p)*，表示第 *pnum* 个多项式对应当前 a_0 值有 *n+expnum* 组分享数据(x_i,y_i)。

c）秘密图像 S 分辨率为 *W×H*，将 S 分解为 *W/4×H* 组 4bit 数据，每组 4 bit 数据 $B_{i,j}$ 作为一个秘密数据 D，使用式（5）计算 $B_{i,j}$ 对应的秘密数据值 $S_{i,j}$。

d）另 $a_0=S_{i,j}$，从 b）中的 $array(pnum,a_0,x_i,y_i)$数组中选择某个多项式下当前 a_0 值对应的 n 组数据(x_i,y_i)，将 n 组数据分享到 n 个分享图像对应位置，并增加随机性控制，包括三个部分：

(a)生成一个[1,pm]的随机整数 r，分享数据将从数组 $array(r,a_0,x_i,y_i)$中选择，这时 *i* 的范围是*[1,n+expnum]*；

(b)从 *n+expnum* 组可选数据中，任意选择 n 组数据作为分享数据，分享数据数组仍然是 $array(r,a_0,x_i,y_i)$，但 *i* 的范围是*[1,n]*；

(c)生成一个*[0,(n-1)]*的随机整数 *cshift*，计算 $c_i=(i+cshift)mod n$，将第 i 组分享数据(x_i,y_i)存放到第 c_i 幅分享图像的对应位置。

e）通过上述过程，将一幅秘密图像 S 分享为 n 幅无意义分享图像，称为分享图像 1-n，每幅分享图像分辨率为 *2W×H*。

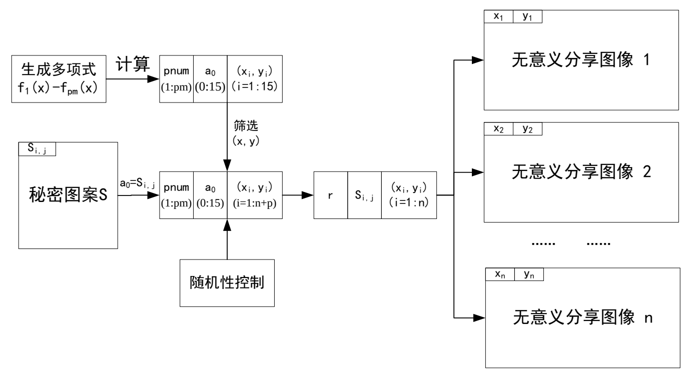


图 7　秘密图像 S 分享为 n 幅分享图像

3.2　从 n 幅分享图像中提取 Cnk 幅秘密图像

从 n 幅分享图像中，任选 k 幅图像，使用拉格朗日插值提取秘密图像。从 n 幅图像中选择 k 幅图像，会有 C_n^k 种情况，一共可提取 C_n^k 幅秘密图像，称为提取的秘密图像 1-C_n^k。提取过程见图 8。具体流程包括：

a）K 幅被选取的分享图像，称为被选取的分享图像 1-k。

b）设每幅分享图像分辨率为 *2W×H*，将每幅图像分解为 *W/4×H* 组 8 bit 数据，每组数据生成分享数据(x_i,y_i)，从 k 幅被选取的分享图像的对应位置共得到 k 组分享数据(x_i,y_i,i=1-k)。

c）将 k 组分享数据(x_i,y_i)，使用式（6）计算拉格朗日插值，得到 a_0。

$$a_0=(\sum_{i=1}^{k}y_i\times\prod_{j=1,j\neq i}^{k}\frac{-x_j}{x_i-x_j})\bmod p \qquad (6)$$

d）另 $S_{i,j}=a_0$，用式（7）计算得到 4 bit 的 $B_{i,j}$，$B_{i,j}$ 为提取秘密图像对应位置的数据。

$$B_{i,j}(b)=(\frac{S_{i,j}}{2^b})\bmod 2 \qquad b=0,1,2,3 \qquad (7)$$

e）当上述过程在整个 k 幅被选取的分享图像上实施后，可提取一幅秘密图像 R_m，m=1-C_n^k。由于 k 组 8 bit 数据，能生成提取的秘密数据为 4 bit，而且被选取的分享图像为 *2W×H*，所以提取的秘密图像 R 分辨率为 *W×H*。

f）使用式（8），可计算提取的秘密图像 R_m 与原始秘密图像 S 的 CDR，R_m 和 S 的分辨率都是 W×H。

$$CDR=\sum_{i=1}^{H}\sum_{j=1}^{W}[s(i,j)\overline{\oplus}r(i,j)]/(W\times H) \qquad (8)$$

4　算法分析与实验结果

4.1　正确性

4.1.1 由秘密图像生成 n 幅分享图像

a）按照 3.1 节中的 a）b）生成数据 $array(pnum,a_0,x_i,y_i)$，表示 pm 个多项式对应每个 a_0 值有 *n+expnum* 组分享数据(x_i,y_i)；

b）将秘密图像 S 中每组 4 bit 数据构成秘密数据值 $S_{i,j}$，另 $a_0=S_{i,j}$，得到一个确定的 a_0；

c）通过随机性控制，获得 n 组分享数据 $array(r,a_0,x_i,y_i)$；

d）将 n 组分享数据存放到第 c_i 幅分享图像的对应位置。

此过程的关键：保证 n 组分享数据来自第 r 个多项式和确定的 a_0 值，即来自于同一个多项式和相同 a_0 值。

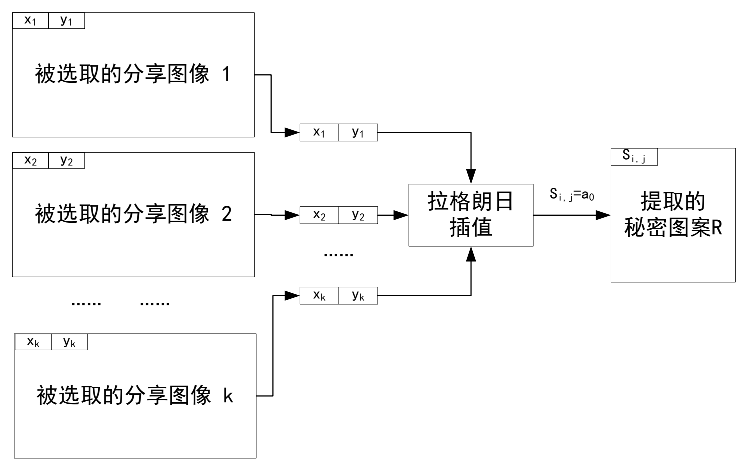


图 8 从分享图像中提取秘密图像

表 2 本文提出的可视加密算法与已有可视加密(VC)算法的对比

算法名称和参考文献	任意(k,n) VC (+)	无像素扩展 (+) / 存在像素扩展 (-)	提取图像的对比度
基于像素扩展的 VC [1-5]	+ 任意(k,n) VC	- 存在像素扩展，随着用户数 n 增加，分享图像会扩展很多倍	提取秘密图像的对比度较好
基于随机网格的 VC [6-13]	+ 任意(k,n) VC	+ 无像素扩展	提取秘密图像的对比度太低
基于图像分块的 VC [14-16]	- 当 n 变化时，图像需要重新划分	+ 无像素扩展	K 个分享图像只能提取出部分秘密图像
本文提出的可视加密算法	+ 任意(k,n) VC	+ 分享图像固定为 2W×H，不随用户数 n 增加而变化	所有提取分享图像的 CDR 为 100%

4.1.2 由分享图像提取秘密图像

a）从 n 幅分享图像中任意选取 k 幅分享图像；

b）从每幅分享图像对应位置获取 8 bit 数据，生成分享数据(x_i,y_i)，共得到 k 组分享数据$(x_i,y_i,i=1\text{-}k)$；

c）使用将 k 组分享数据，使用式（6）计算拉格朗日插值，得到 a_0；

d）将 a_0 转换为 4 bit 数据作为提取的秘密数据，构成提取的秘密图像。

提取 a_0 正确性：k 组分享数据来自于同一多项式和相同的 a_0 值，通过拉格朗日计算，必然得到正确的 a_0。

由于提取的每个 a_0 都正确，**提取的秘密图像必然正确**。

4.2 实验结果

BUPT BUPT

BUPT BUPT

(a) 提取秘密图像 1　　(b) 提取秘密图像 2

BUPT BUPT

BUPT BUPT

(c) 提取秘密图像 3　　(d) 提取秘密图像 4

图 9 图 2(a)做为秘密图像 S，提取 C_4^3 幅秘密图像

另图 2(a)为秘密图像 S，采用 3.1 节中的算法生成 4 幅分享图像（图 6），从 4 幅分享图像中任选 3 幅图像，可有 4 种组合，对每种组合采用 3.2 节中的算法可提取 1 幅秘密图像，共可提取 4 幅秘密图像，如图 9 所示。

BIGC BIGC

BIGC BIGC

(a) 提取秘密图像 1　　(b) 提取秘密图像 2

BIGC BIGC

BIGC BIGC

(c) 提取秘密图像 3　　(d) 提取秘密图像 4

图 10 图 2(b)做为秘密图像 S，提取 C_4^3 幅秘密图像

其中，使用分享图像 1,2,3 提取图 9(a)；使用分享图像 1,2,4 提取图 9(b)；使用分享图像 1,3,4 提取图 9(c)；使用分享图像 2,3,4 提取图(d)。使用式（8，计算 4 幅提取的秘密图像 CDR 分别为：1, 1, 1, 1。）

另图 2(b)为秘密图像 S，采用 3.1 中的算法生成 4 幅分享图像，从 4 幅分享图像中任选 3 幅图像，可有 4 种组合，对每种组合采用 3.2 节中的算法可提取 1 幅秘密图像，共可提取 4 幅秘密图像，如图 10 所示。使用式（8），计算 4 幅提取的秘密图像 CDR 分别为：1, 1, 1, 1。

从图 9、10 和 CDR 结果可看出，对生成的分享图像，使用拉格朗日插值提取秘密图像，不会产生任何误码，提取正确率均为 100%。

4.3 本算法与已有算法的对比

表 2 列出本文提出的可视加密算法与已有可视加密(VC)算法的对比。

从表 2 可看出，本节提出的可视加密算法可实现任意(k,n)可视加密(VC)，并且当原始秘密图像为 W×H 时，生成的分享图像分辨率固定为 2W×H，分享图像分辨率不随用户数 n 增加而变化。所以，在所有算法中，本文提出的可视加密算法拥有最好的性能。

5 结束语

本文提出一种基于 Shamir 秘密分享的高质量(k,n)可视加密算法。使用该算法，将一幅二进制秘密图像隐藏在 n 幅无意义分享图像中。从 n 幅无意义分享图像中，任意选取 k 幅分享图像，使用拉格朗日插值可提取秘密图像。

本算法的主要优点是应用 Shamir 秘密分享来实现(k,n)可视加密，该算法不需要码书，不会造成无限制的像素扩展。实验结果显示，该算法能实现(k,n)可视加密，提取秘密图像的提取正确率能保证 100%。

参考文献：

[1] Naor M, Shamir A. Visual cryptography [C]// Proc of Workshop on the Theory and Application of Cryptographic Techniques. Italy: Springer, 1995: 1-12.

[2] Ateniese G, Blundo C, Santis A, *et al.* Extended capabilities for visual cryptography [J]. Theoretical Computer Science, 2001, 250 (1-2): 143–161.

[3] Liu Feng, Wu Chuankun, Lin Xijun. Step construction of visual cryptography schemes [J]. IEEE Trans on Information Forensics and Security, 2010, 5 (1): 27-38.

[4] Hou Y C, Quan Zenyu, Liao H Y. New designs for friendly visual cryptography scheme [J]. International Journal of Information and Electronics Engineering, 2015, 5 (1): 15-20.

[5] Yan Xuehu, Lu Yuliang, Chen Yuxin, *et al.* Secret image sharing based on error-correcting codes [C]// Proc of the 3rd IEEE International Conference on Big Data Security on Cloud. [S. l.] : Institute of Electrical and Electronics Engineers Inc, 2017: 86-89.

[6] Kafri O, Keren E. Encryption of pictures and shapes by random grids [J]. Optics Letters. 1987, 12 (6): 377-379.

[7] Chen T H, Tsao K H. Visual secret sharing by random grids revisited [J]. Pattern Recognition. 2009, 42 (9): 2203-2217.

[8] Chen T H, Tsao K H. Threshold visual secret sharing by random grids [J]. Journal of Systems and Software, 2011, 84 (7): 1197-1208.

[9] Wu Xiaotian, Sun Wei. Random grid-based visual secret sharing for general access structures with cheat-preventing ability [J]. Journal of Systems and Software, 2011, 85 (5): 1119-1134.

[10] Wu X, Sun W. Visual secret sharing for general access structures by random grids [J]. Iet Information Security, 2012, 6 (4): 299-309.

[11] Ou Duanhao, Wu Xiaotian, Dai Lu, *et al.* Improved tagged visual cryptograms by using random grids [J]. Lecture Notes in Computer Science, 2014, 8389: 79-94.

[12] Yan Xuehu, Lu Yuliang, Liu Lintao, *et al.* Progressive visual secret sharing for general access structure with multiple decryptions [C]// Proc of the 8th International Conference on Information Technology in Medicine and Education. [S. l.] : Institute of Electrical and Electronics Engineers Inc, 2016: 668-673.

[13] Rabari D K, Meghrajani Y K. Lock and key share-based random grid visual secret sharing scheme for grayscale and color images with two decoding options [C]// Proc of ISEA Asia Security and Privacy Conference. India: Institute of Electrical and Electronics Engineers Inc, 2017: 1-5.

[14] Hou Y C, Quan Zenyu, Tsai C F, *et al.* Block-based progressive visual secret sharing [J]. Information Sciences, 2013, 233 (2): 290-304.

[15] Hou Y C, Quan Zenyu, Tsai C F, *et al.* Cheating immune block-based progressive visual cryptography [J]. Lecture Notes in Computer Science, 2014, 8389: 95-108.

[16] Roy R, Bandyopadhyay S, Kandar S, *et al.* A novel 3-4 image secret sharing scheme [C]// Proc of International Conference on Advances in Computing, Communications and Informatics. India: Institute of Electrical and Electronics Engineers Inc, 2015: 2072-2075.

[17] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22 (11): 612-613.